

THE SCHUR-WIELANDT THEORY FOR CENTRAL S-RINGS

GANG CHEN, MIKHAIL MUZYCHUK, AND ILYA PONOMARENKO

ABSTRACT. Two basic results on the S-rings over an abelian group are the Schur theorem on multipliers and the Wielandt theorem on primitive S-rings over groups with a cyclic Sylow subgroup. None of these theorems is directly generalized to the non-abelian case. Nevertheless, we prove that they are true for the central S-rings, i.e., for those which are contained in the center of the group ring of the underlying group (such S-rings naturally arise in the supercharacter theory). We also generalize the concept of a B-group introduced by Wielandt, and show that any Camina group is a generalized B-group whereas with few exceptions, no simple group is of this type.

1. INTRODUCTION

A *Schur ring* or *S-ring* over a finite group G can be defined as a subring of the group ring $\mathbb{Z}G$ that is a free \mathbb{Z} -module spanned by a partition of G closed under taking inverse and containing the identity e of G as a class (see Section 2 for details). The S-ring theory was initiated by Schur [13] and then developed by Wielandt [14] who wrote in [15] that S-rings provide one “of three major tools” to study a group action.¹

Until recently, the focus was on studying S-rings over abelian groups and the main applications of this theory were connected with algebraic combinatorics problems [12]. However, as it was observed in [9], the supercharacter theory developed to study group representations, is nothing else than the theory of commutative S-rings of a special form that we call here *central*.

Definition 1.1. *An S-ring over a group G is said to be central if it is contained in the center $\mathcal{Z}(\mathbb{Z}G)$ of the group ring $\mathbb{Z}G$.*

An example of such a ring is obtained from any permutation group K such that

$$G \operatorname{Inn}(G) \leq K \leq \operatorname{Sym}(G),$$

where $\operatorname{Inn}(G)$ is the inner automorphism group of G ; the corresponding partition of G is formed by the orbits of the stabilizer of e in K . In the special case when $K = \operatorname{Sym}(G)$, this produces the *trivial* central S-ring $\mathbb{Z}e + \mathbb{Z}\underline{G}$, where \underline{G} is the sum of all elements of G . On the other hand, if $K = G \operatorname{Inn}(G)$, the orbits are the conjugacy classes of G ; this shows that $\mathcal{Z}(\mathbb{Z}G)$ is a central S-ring. In particular, any S-ring over an abelian group is central. The main goal of the present paper is to extend the basic results on S-rings from abelian case to the central one.

The work of the first author was Financially supported by self-determined research funds of CCNU (No.CCNU15A02031) from the colleges basic research and operation of MOE. The work of the third author was partially supported by the RFBR Grant 14-01-00156.

¹The two other tools are the representation theory and the method of invariant relations.

The Schur theorem on multipliers is a fundamental statement in the theory of S-rings over abelian groups. To explain it, given an integer m coprime to $|G|$, we define a permutation on the elements of the group G by

$$\sigma_m : G \rightarrow G, x \mapsto x^m.$$

It permutes also the conjugacy classes of G , and so induces a linear isomorphism of the ring $\mathcal{Z}(\mathbb{Z}G)$. If the group G is abelian, then $\sigma_m \in \text{Aut}(G)$, $\mathcal{Z}(\mathbb{Z}G) = \mathbb{Z}G$ and the Schur theorem on multipliers states that σ_m is a Cayley automorphism of every S-ring over G . Our first result shows that in the nonabelian case, σ_m is still an automorphism (but not a Cayley one) of any central S-ring over G .

Theorem 1.2. *Let \mathcal{A} be a central S-ring over a group G , and let m be an integer coprime to $|G|$. Then $\sigma_m(\mathcal{A}) = \mathcal{A}$ and $\sigma_m|_{\mathcal{A}} \in \text{Aut}(\mathcal{A})$.*

Based on this result for the abelian case, Wielandt generalized the Schur theorem on primitive groups having a regular cyclic subgroup. In fact, the Wielandt proof shows that if G is an abelian group of composite order that has a cyclic Sylow subgroup, then no proper S-ring over G is primitive.² The following statement establishes “a central version” of the Wielandt theorem.

Theorem 1.3. *Let \mathcal{A} be a nontrivial central S-ring over a group G of composite order. Suppose that G has a normal cyclic Sylow p -subgroup. Then \mathcal{A} is imprimitive.*

Following [14], a finite group G is called a B-group if every primitive group containing a regular subgroup isomorphic to G is 2-transitive. It should be remarked that most of the B-groups G mentioned in [14] satisfy a priori a stronger condition: no nontrivial S-ring over G is primitive. In this sense, the following definition seems to be quite natural. In what follows, we say that a central S-ring over G is *proper* if it lies strictly between $\mathcal{Z}(\mathbb{Z}G)$ and the trivial S-ring over G .

Definition 1.4. *A group G is called a generalized B-group if no proper central S-ring over G is primitive.*

Clearly, every B-group is also a generalized one. The converse statement is not true; see Subsection 5.2. A nontrivial example of a generalized B-group is given in Theorem 1.3. The following statement gives a family of generalized B-groups; we don’t know whether they are B-groups. Below, under a *Camina* group, we mean a group G that has a proper nontrivial normal subgroup H such that each H -coset distinct from H is contained in a conjugacy class of G (in other terms, (G, H) is a Camina pair).³

Theorem 1.5. *Any Camina group is a generalized B-group.*

The class of the Camina groups includes, in particular, all Frobenius and extraspecial groups; see [3]. Thus, by Theorem 1.5, we obtain the following statement.

Corollary 1.6. *Any Frobenius or extra-special group is a generalized B-group. ■*

²The primitivity concept in S-ring theory plays the same role as the simplicity in group theory.

³To simplify the presentation, we use the term “Camina group” not only in the case where (G, G') is a Camina pair.

The last result of the present paper shows that with a few possible exceptions, no simple group is a generalized B-group. The proof is based on the Schur theorem on multipliers and the characterization of rational simple groups given in [7].

Theorem 1.7. *A generalized B-group G is not simple unless $|G| \leq 3$, or $G \cong \text{Sp}(6, 2)$ or $\text{O}^+(8, 2)$.*⁴

For the reader convenience, we collect the basic facts on S-rings in Section 2. The proofs of Theorems 1.2 and 1.3 are contained in Sections 3 and 4, respectively. The results concerning generalized B-groups are in Section 5.

Notation.

As usual, \mathbb{Z} , \mathbb{Q} and \mathbb{C} denote the ring of integers and the fields of rationals and complex numbers, respectively.

The identity of a group G is denoted by e ; the set of non-identity elements in G is denoted by $G^\#$.

The set of conjugacy classes of G is denoted by $\text{Cla}(G)$.

Let $X \subseteq G$. The subgroup of G generated by X is denoted by $\langle X \rangle$; we also set $\text{rad}(X) = \{g \in G : gX = Xg = X\}$.

The element $\sum_{x \in X} x$ of the group ring $\mathbb{Z}G$ is denoted by \underline{X} .

For an integer m , we set $X^{(m)} = \{x^m : x \in X\}$ and $\underline{X}^{(m)} = \underline{X^{(m)}}$.

The group of all permutations of the elements of G is denoted by $\text{Sym}(G)$.

The additive and multiplicative groups of the ring $\mathbb{Z}/(n)$ are denoted by \mathbb{Z}_n and \mathbb{Z}_n^* , respectively.

2. PRELIMINARIES

Let G be a finite group. A subring \mathcal{A} of the group ring $\mathbb{Z}G$ is called a *Schur ring* (*S-ring*, for short) over G if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of G such that

- (S1) $\{e\} \in \mathcal{S}$,
- (S2) $X \in \mathcal{S} \Rightarrow X^{-1} \in \mathcal{S}$,
- (S3) $\mathcal{A} = \text{Span}\{\underline{X} : X \in \mathcal{S}\}$.

In particular, for all $X, Y, Z \in \mathcal{S}$ there is a nonnegative integer c_{XY}^Z such that

$$\underline{X}\underline{Y} = \sum_{Z \in \mathcal{S}} c_{XY}^Z \underline{Z},$$

these integers are the structure constants of \mathcal{A} with respect to the linear base $\{\underline{X} : X \in \mathcal{S}\}$. The number $\text{rk}(\mathcal{A}) = |\mathcal{S}|$ is called the *rank* of \mathcal{A} .

Let \mathcal{A}' be an S-ring over a group G' . Under a *Cayley isomorphism* from \mathcal{A} to \mathcal{A}' , we mean a group isomorphism $f : G \rightarrow G'$ such that $\mathcal{S}(\mathcal{A})^f = \mathcal{S}(\mathcal{A}')$. This is a special case of the ordinary *isomorphism*; by definition, it is a bijection $f : G \rightarrow G'$ that induces a ring isomorphism from \mathcal{A} to \mathcal{A}' taking \underline{X} to $\underline{X'}$ for all $X \in \mathcal{S}$, where $X' = X^f$.

The classes of the partition \mathcal{S} are called the *basic sets* of the S-ring \mathcal{A} . Any union of them is called an \mathcal{A} -set. Thus, $X \subseteq G$ is an \mathcal{A} -set if and only if $\underline{X} \in \mathcal{A}$. The set of all \mathcal{A} -sets is closed with respect to taking inverse and product. Any subgroup of G that is an \mathcal{A} -set, is called an \mathcal{A} -subgroup of G or \mathcal{A} -group. With each \mathcal{A} -set X , one can naturally associate two \mathcal{A} -groups, namely $\langle X \rangle$ and $\text{rad}(X)$ (see Notation).

⁴In fact, we do not know whether two simple groups from Theorem 1.7 are generalized B-groups.

The S-ring \mathcal{A} is called *primitive* if the only \mathcal{A} -groups are e and G , otherwise this ring is called *imprimitive*.

We will use the following statement proved in [14, Proposition 22.3]. Below for a function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ and an element $\xi = \sum_g a_g g$ of the ring $\mathbb{Z}G$, we set $f[\xi] = \sum_g f(a_g)g$.

Lemma 2.1. *Let \mathcal{A} be an S-ring, $f : \mathbb{Z} \rightarrow \mathbb{Z}$ an arbitrary function and $\xi \in \mathcal{A}$. Then $f[\xi] \in \mathcal{A}$.* ■

The important special case is when $f(a) = 1$ or 0 depending on whether $a \neq 0$ or $a = 0$. Then $f[\xi] = \underline{X}$, where X is the support of ξ , and we refer to Lemma 2.1 as to the Schur-Wielandt principle.

3. THE SCHUR THEOREM ON MULTIPLIERS

Proof of Theorem 1.2. Since obviously $\sigma_{mm'} = \sigma_m \sigma_{m'}$ for all m and m' , without loss of generality, we can assume that m is a prime. We need the following auxiliary lemma.

Lemma 3.1. *Let $X \in \text{Cla}(G)$ and p an arbitrary prime. Then*

$$\underline{X}^p = \sum_{Y \in \text{Cla}(G)} a_Y \underline{Y}$$

for some nonnegative integers a_Y 's. Moreover,

$$a_Y |Y| = \begin{cases} |X| \pmod{p}, & \text{if } Y = X^{(p)}, \\ 0 \pmod{p}, & \text{if } Y \neq X^{(p)}. \end{cases}$$

Proof. The first statement follows from the fact that $\mathcal{Z}(\mathbb{Z}G)$ is an S-ring. To prove the second one, set

$$T_Y = \{(x_1, \dots, x_p) \in X^p : x_1 \cdots x_p \in Y\}.$$

Clearly, $(T_Y)^G = T_Y$. Since also $(x_1 x_2 \cdots x_p)^{x_1} = x_2 \cdots x_p x_1$, the set T_Y is invariant with respect to the cyclic shift $\pi : (x_1, x_2, \dots, x_p) \mapsto (x_2, \dots, x_p, x_1)$. Moreover, since p is prime, we have

$$|(x_1, \dots, x_p)^{\langle \pi \rangle}| = 1 \text{ or } p.$$

However, $|(x_1, \dots, x_p)^{\langle \pi \rangle}| = 1$ if and only if $x_1 = \cdots = x_p$, which is possible only if $Y = X^{(p)}$; in the latter case, the group $\langle \pi \rangle$ has exactly $|X|$ orbits of the form $\{(x, \dots, x)\}$, $x \in X$. Taking into account that T_Y is a disjoint union of $\langle \pi \rangle$ -orbits, we have

$$|T_Y| = |X|\delta + pu$$

where $\delta = \delta_{Y, X^{(p)}}$ is the Kronecker delta and u is the number of the $\langle \pi \rangle$ -orbits of size p . Thus, the required statement follows because $a_Y |Y| = |T_Y|$. ■

Let us continue the proof of the theorem. Since $p := m$ is coprime to $|G|$, the mapping

$$\underline{X} \mapsto \underline{X}^{(p)}, \quad X \in \text{Cla}(G),$$

is a bijection. It induces a linear isomorphism of the ring $\mathcal{Z}(\mathbb{Z}G)$; the image of the element ξ under this isomorphism is denoted by $\xi^{(p)}$. From Lemma 3.1, it follows

that $\underline{X}^p = \underline{X}^{(p)} \pmod{p}$; here, we make use of the fact that $|X^{(p)}| = |X|$ for all X . Therefore,

$$(1) \quad \xi^{(p)} = f[\xi^p] \quad \text{for all } \xi \in \mathcal{Z}(\mathbb{Z}G).$$

where $f(a)$ is the remainder in the division of a by p .

To prove the first part of the theorem, let $X \in \mathcal{S}(\mathcal{A})$. Then X is a union of some classes $X_i \in \text{Cla}(G)$, $i \in I$. Thus, by (1), we have

$$(2) \quad \sigma_p(\underline{X}) = \underline{X}^{(p)} = \sum_{i \in I} \underline{X}_i^{(p)} = \sum_{i \in I} f[\underline{X}_i^p] = f[\sum_{i \in I} \underline{X}_i^p] = f[(\sum_{i \in I} \underline{X}_i)^p] = f[\underline{X}^p].$$

However, by Lemma 2.1, the right-hand side belongs to \mathcal{A} . Therefore $\sigma_p(\underline{X}) \in \mathcal{A}$ and $X^{(p)}$ is an \mathcal{A} -set. Moreover, suppose that it contains a proper basic set Y . By the Dirichlet Theorem, one can find a prime p' such that $pp' \equiv 1 \pmod{n}$, where $n = |G|$. Now, the above argument shows that $Y^{(p')}$ is a proper \mathcal{A} -subset of X . Thus $X^{(p)} \in \mathcal{S}(\mathcal{A})$ and so $\sigma_p(\mathcal{A}) = \mathcal{A}$.

To prove the second part of the theorem, it suffices to verify that σ_m induces a ring isomorphism of $\mathcal{Z}(\mathbb{Z}G)$: then it is, obviously, an S-ring isomorphism of $\mathcal{Z}(\mathbb{Z}G)$ that takes \mathcal{A} to itself, and hence it is an isomorphism of \mathcal{A} , as required. To do this, without loss of generality, we can assume that $p > 2n$ (for otherwise, by the Legendre theorem, there exists a prime $q > 2n$ such that $q \equiv p \pmod{n}$), and then, obviously, $\xi^{(q)} = \xi^{(p)}$ for all $\xi \in \mathcal{A}$. We have to prove that

$$(3) \quad c_{X^{(p)}Y^{(p)}}^{Z^{(p)}} = c_{XY}^Z$$

for all $X, Y, Z \in \text{Cla}(G)$, where the numbers in the both sides are the structure constants of the S-ring $\mathcal{Z}(\mathbb{Z}G)$. Since this ring is commutative and p is prime, formula (2) implies that

$$\underline{X}^{(p)} \underline{Y}^{(p)} \equiv \underline{X}^p \underline{Y}^p = (\underline{X} \underline{Y})^p = \left(\sum_Z c_{XY}^Z \underline{Z} \right)^p \equiv \sum_Z c_{XY}^Z \underline{Z}^{(p)} \pmod{p}.$$

Thus the relation (3) is true modulo p . Since $p > 2n$, we are done. \blacksquare

There is an alternative way to prove the second part of Theorem 1.2. It is related to the action of the group \mathbb{Z}_n^* on the set $\text{Irr}(\mathcal{A})$ of all irreducible \mathbb{C} -characters of the S-ring \mathcal{A} , where as before, we can assume that $\mathcal{A} = \mathcal{Z}(\mathbb{Z}G)$. Let ε be an n -th primitive complex root of unity. Then each $m \in \mathbb{Z}_n^*$ determines an automorphism τ_m of the cyclotomic field $\mathbb{Q}(\varepsilon)$, which sends ε to ε^m . It follows that for any $\chi \in \text{Irr}(G)$, the function $\chi^{\tau_m}(g) := (\chi(g))^{\tau_m}$, $g \in G$, is also an irreducible character of G and

$$\chi^{\tau_m}(g) = \chi(g^m)$$

(see [11, Proposition 3.16]). The primitive idempotents of \mathcal{A} coincide with the central primitive idempotents of the group algebra $\mathbb{Q}(\varepsilon)[G]$ which, in turn, are in a one-to-one correspondence with the irreducible characters of G . More precisely, if e_χ is the idempotent corresponding to $\chi \in \text{Irr}(G)$, then

$$e_\chi = \frac{1}{|G|} \sum \chi(g) g^{-1}.$$

A direct computation shows that $\sigma_m(e_\chi) = e_{\chi^{\tau_m}}$. Thus, σ_m permutes the primitive idempotents of \mathcal{A} . This implies that σ_m is an automorphism of \mathcal{A} , as required. We

note that the above formula shows that there is a natural one-to-one correspondence between the $\text{Irr}(G)$ and $\text{Irr}(\mathcal{A})$. More precisely,

$$(4) \quad \text{Irr}(\mathcal{A}) = \left\{ \frac{1}{\chi(1)} \chi|_{\mathcal{A}} : \chi \in \text{Irr}(G) \right\}.$$

Given a set $X \subseteq G$, denote by $\text{tr}(X)$ the union of the sets $X^{(m)}$, where m runs over the integers coprime to $n = |G|$; it is called the *trace* of X . Let \mathcal{A} be a central S-ring over G . Then from Theorem 1.2, it follows that $\underline{\text{tr}(X)} \in \mathcal{A}$ for all $X \in \mathcal{S}(\mathcal{A})$. Therefore,

$$\text{tr}(\mathcal{A}) = \text{Span}\{\underline{\text{tr}(X)} : X \in \mathcal{S}(\mathcal{A})\}$$

is a submodule of \mathcal{A} . It is easily seen that it consists of all fixed points of the natural action of the group $\{\sigma_m : (m, n) = 1\}$ on \mathcal{A} . Thus, $\text{tr}(\mathcal{A})$ is an S-ring, which is obviously central; it is called the *rational closure* of the S-ring \mathcal{A} . It should be noted that our definitions agreed with the relevant definitions in the abelian case. The following statement immediately follows from the fact that the $\text{tr}(H) = H$ for any group $H \leq G$.

Proposition 3.2. *Let \mathcal{A} be a central S-ring over G . Then \mathcal{A} is primitive if and only if so is $\text{tr}(\mathcal{A})$.* ■

We say that a central S-ring is *rational* if it coincides with its rational closure, or equivalently, if each of its basic sets is rational. The following statement justified the term “rational”.

Theorem 3.3. *Let \mathcal{A} be a central S-ring over a group G . Then it is rational if and only if $\pi(\underline{X}) \in \mathbb{Q}$ for all $\pi \in \text{Irr}(\mathcal{A})$ and all $X \in \mathcal{S}(\mathcal{A})$.*

Proof. Let m be an integer coprime to $n = |G|$. Since any character $\pi \in \text{Irr}(\mathcal{A})$ is equal to the restriction to \mathcal{A} of a suitable character $\chi \in \text{Irr}(G)$, from relation (4) it follows that

$$(5) \quad \pi(\underline{X})^{\tau_m} = \pi(\underline{X}^{(m)}), \quad X \in \mathcal{S}(\mathcal{A}),$$

where τ_m is the above defined automorphism of the field $\mathbb{Q}(\varepsilon)$. If the S-ring \mathcal{A} is rational, then the right-hand side of this equality does not depend on the choice of m . So the number $\pi(\underline{X})^\tau$ does not depend on the automorphism τ of $\mathbb{Q}(\varepsilon)$. Thus, $\pi(\underline{X}) \in \mathbb{Q}$.

Assume now that $\pi(\underline{X}) \in \mathbb{Q}$ for all $\pi \in \text{Irr}(\mathcal{A})$ and $X \in \mathcal{S}(\mathcal{A})$. Then from (5) it follows that $\pi(\underline{X}) = \pi(\underline{X}^{(m)})$ for all integers m coprime to n and all characters $\pi \in \text{Irr}(\mathcal{A})$. This implies that

$$\underline{X} = \sum_{\pi \in \text{Irr}(\mathcal{A})} \pi(\underline{X}) e_\pi = \sum_{\pi \in \text{Irr}(\mathcal{A})} \pi(\underline{X}^{(m)}) e_\pi = \underline{X}^{(m)},$$

where e_π is the primitive idempotent corresponding to the character π . Thus, the S-ring \mathcal{A} is rational. ■

4. PROOF OF THEOREM 1.3

By the theorem hypothesis, G has a normal Sylow p -subgroup $P \cong \mathbb{Z}_{p^n}$. So by the Schur-Zassenhaus theorem, $G = PK$, where K is a Hall p' -subgroup of G . In what follows, we denote by H the unique subgroup of P of order p .

Lemma 4.1. *Let $x \in G$ be such that $Hx \not\subseteq x^G$. Then $x \in C_G(P)$.*

Proof. The element x acts by conjugation as an automorphism of the cyclic group P . Therefore, there exists an integer m coprime to p such that $h^x = h^m$ for all $h \in P$. Rewriting this equality as $x^h = xh^{1-m}$, we obtain

$$x^G \supseteq x^P \supseteq P^{(1-m)}x.$$

Since $P^{(1-m)}$ is a subgroup of P and $x^G \not\supseteq xH$, this implies that $P^{(1-m)} = e$. Thus, $x^h = x$ for all $h \in P$, which means that $x \in C_G(P)$. \blacksquare

Suppose on the contrary that the S-ring \mathcal{A} is primitive. Take a nontrivial basic set X , which intersects H nontrivially. Then $\langle X \rangle \neq H$: indeed, otherwise $\langle X \rangle = H$ by the primitivity of \mathcal{A} and $n = p$ is a prime in contrast to the hypothesis. This proves the second part of the following relations (the first one follows from the choice of X):

$$(6) \quad X \cap H \neq \emptyset \quad \text{and} \quad X \setminus H \neq \emptyset \quad \text{and} \quad \langle X \cap H \rangle \leq \text{rad}(X \setminus H).$$

To prove the third one, set $X_0 = \{x \in X : xH \not\subseteq X\}$. Then from Lemma 4.1 it follows that

$$(7) \quad (X_0)^{(p)} \subseteq P^{(p)}K \subsetneq G.$$

Moreover, it is easily seen that the sets X_0 and $X \setminus X_0$ are unions of some conjugacy classes of G . For these classes, we can refine Lemma 3.1 as follows.

Lemma 4.2. *For any class $Y \in \text{Cla}(G)$, we have*

$$\underline{Y}^p \equiv \begin{cases} \underline{Y}^{(p)} \pmod{p}, & \text{if } Y \subseteq C_G(P), \\ 0 \pmod{p}, & \text{if } Y \not\subseteq C_G(P). \end{cases}$$

Proof. The group $C := C_G(P)$ is obviously normal in G . Therefore,

$$Y \subseteq C \quad \text{or} \quad Y \cap C = \emptyset.$$

Suppose first that $Y \cap C = \emptyset$. Since $H \trianglelefteq G$, we have $yH = Hy$ for all $y \in Y$. Denote by S a full system of representatives of the family $\{Hy : y \in Y\}$. Then, since $|H| = p$, we have

$$\underline{Y}^p = \left(\sum_{y \in S} Hy \right)^p \equiv \underline{H}^p \underline{S}^p \equiv 0 \pmod{p},$$

as required. Let now $Y \subseteq C$. Then Y is a normal subset of C , i.e. $Y^G = Y$. Since the group C is a direct product of P and $O_{p'}(C)$, each normal subset of C is the disjoint union of gY_g , $g \in P$, where Y_g is a normal subset of $O_{p'}(C)$. Now

$$(8) \quad \underline{Y}^{(p)} = \sum_{g \in P} g \underline{Y_g}^{(p)} = \sum_{g \in P} g^p \underline{Y_g}^{(p)}.$$

Moreover, since Y_g is contained in the p' -subgroup $O_{p'}(C)$, by Lemma 3.1 we obtain

$$(9) \quad \underline{Y_g}^{(p)} = \underline{Y_g}^{(p)} \equiv \underline{Y_g}^p \pmod{p}.$$

Thus, from (8) and (9), it follows that

$$\underline{Y}^p \equiv \sum_{g \in P} (g \underline{Y_g})^p = \sum_{g \in P} g^p \underline{Y_g}^p \equiv \sum_{g \in P} g^p \underline{Y_g}^{(p)} = \underline{Y}^{(p)} \pmod{p}$$

as required. \blacksquare

To complete the proof of the third relation in (6), suppose on the contrary that the set X_0 is not empty. Then, if X is the union of conjugacy classes X_i , $i \in I$, then by Lemma 4.2, we have

$$(10) \quad \underline{X}^p = \left(\sum_{i \in I} \underline{X}_i \right)^p = \sum_{i \in I} \underline{X}_i^p = \sum_{i \in I_0} \underline{X}_i^{(p)} \pmod{p},$$

where $I_0 = \{i \in I : X_i \subseteq X_0\}$. Moreover, by Lemma 4.1, given $x, y \in X_0$, the equality $x^p = y^p$ holds if and only if $y \in Hx$. Since also

$$1 \leq |Hx \cap X_0| \leq p-1$$

for all $x \in X_0$, the coefficient at $x^p \in G$ in the right-hand sum of (10) is between 1 and $p-1$. Thus,

$$\xi := f[\underline{X}^p]$$

is a non-zero element of the S-ring \mathcal{A} , where f is the function used in (1). By the Schur-Wielandt principle, this implies that the support Y of the element ξ is an \mathcal{A} -set. Therefore, $\langle Y \rangle$ is an \mathcal{A} -subgroup of G . This subgroup is proper: $\langle Y \rangle \neq G$ by (7) and $\langle Y \rangle \neq e$, because $X_0 \neq \emptyset$. But this contradicts the primitivity of the S-ring \mathcal{A} .

Thus, all the relations in (6) are true. To complete the proof, we make use of the following theorem on separating subgroup proved in [6].

Theorem 4.3. *Let \mathcal{A} be an S-ring over a group G . Suppose that $X \in \mathcal{S}(\mathcal{A})$ and $H \leq G$ satisfy relations (6). Then $X = \langle X \rangle \setminus \text{rad}(X)$ and $\text{rad}(X) \leq H \leq \langle X \rangle$. ■*

Now, since $\text{rad}(X)$ and $\langle X \rangle$ are \mathcal{A} -groups, the primitivity assumption implies that $\text{rad}(X) = e$ and $\langle X \rangle = G$. By Theorem 4.3, this implies that $X = G \setminus e$. This means that $\text{rk}(\mathcal{A}) = 2$, i.e., the S-ring \mathcal{A} is trivial. Contradiction.

5. GENERALIZED B-GROUPS

5.1. Proof of Theorem 1.5. Let G be a Camina group. Then it has a normal subgroup H such that (G, H) is a Camina pair. Let \mathcal{A} be a proper central primitive S-ring over G . Take a set $X \in \mathcal{S}(\mathcal{A})$ that contains a nonidentity element of H . It follows from the primitivity of \mathcal{A} that

$$(11) \quad \text{rad}(X) = e \quad \text{and} \quad \langle X \rangle = G.$$

In particular, the first two relations in (6) hold. Next, the set X is a union of some conjugacy classes of G as the S-ring \mathcal{A} is central. By the definition of a Camina pair, we have

$$xH = Hx \subseteq X \setminus H$$

for all $x \in X \setminus H$. This proves the third relation in (6). Thus, $X = \langle X \rangle \setminus \text{rad}(X)$ by Theorem 4.3. By (11), this implies that $X = G \setminus e$ and hence $\text{rk}(\mathcal{A}) = 2$. The latter means that the S-ring \mathcal{A} is not proper. Contradiction. ■

5.2. A generalized B-group, which is not a B-group. Let $p > 3$ be a prime congruent to 3 modulo 4, and let G be the extraspecial group of order p^3 and exponent p . Then there exists a skew Hadamard difference set X in the group G ; see [8]. This exactly means that $Y := X^{-1}$ is equal to $G^\# \setminus X$ and

$$\underline{XY} = |X|e + \frac{|X| - 1}{2}(\underline{X} + \underline{Y}).$$

Therefore, the module $\mathcal{A} = \text{Span}\{e, \underline{X}, \underline{Y}\}$ is a subring of $\mathbb{Z}G$ that satisfies the conditions (S1), (S2), and (S3) with $\mathcal{S} = \{e, X, Y\}$. Thus, \mathcal{A} is an S-ring of rank 3 over G . This S-ring is, obviously, primitive. Since it is also proper, G is not a B-group. On the other hand, it is a generalized B-group by Corollary 1.6.

5.3. Simple groups. According to [7], a group G is said to be *rational* if the number $\chi(g)$ is rational for all $\chi \in \text{Irr}(G)$ and all $g \in G$. Finite simple rational groups were characterized in Corollary B1 of that paper as follows: a noncyclic simple group G is rational if and only if $G \cong \text{Sp}(6, 2)$ or $\text{O}^+(8, 2)'$.

Proof of Theorem 1.7. Let G be a finite simple group other than $\text{Sp}(6, 2)$ or $\text{O}^+(8, 2)'$. Without loss of generality, we can assume that G is not cyclic. Then by the above characterization of rational groups, G is not rational and has two elements x and y of distinct orders. Then the orders of x^m and y^m are also distinct for all integers m coprime to $|G|$. This implies that the order of any element of $\text{tr}(x^G)$ does not equal the order of any element of $\text{tr}(y^G)$. So,

$$(12) \quad \text{tr}(x^G) \neq \text{tr}(y^G).$$

Therefore, the rational closure $\text{tr}(\mathcal{A})$ of the S-ring $\mathcal{A} = \mathcal{Z}(\mathbb{Z}G)$ is of rank at least 3. On the other hand, $\text{tr}(\mathcal{A}) \neq \mathcal{A}$, for otherwise the irreducible characters of \mathcal{A} are rational valued (Theorem 3.3) and then G is a rational group. Thus, $\text{tr}(\mathcal{A})$ is a proper central S-ring. It is primitive because so is \mathcal{A} (Proposition 3.2). Therefore G can not be a generalized B-group. ■

5.4. AS-free groups. According to [1], a transitive permutation group is called *AS-free* if it preserves no nontrivial symmetric association scheme. From Theorem 17 of that paper, it follows that given a nonabelian simple group G , the permutation group on G defined by

$$K = \langle G_{\text{right}}, \text{Aut}(G), \sigma \rangle,$$

is AS-free, where G_{right} is the group of all right translations of G and σ is a permutation of G that takes g to g^{-1} , $g \in G$. It is easily seen that the orbits of the stabilizer of e in K are the basic sets of a central S-ring \mathcal{A} over G . Thus, using the above result one can get another proof that G is not a generalized B-group whenever $\mathcal{A} \neq \mathcal{Z}(\mathbb{Z}G)$. However, in general, the latter inequality is not true, e.g., for the group $\text{Sp}(6, 2)$.

5.5. Miscellaneous. Let G be a finite group having a relatively prime conjugacy class (examples of such groups can be found, e.g., in [4]). Denote by \mathcal{X} the association scheme of the permutation group $G \text{ Inn}(G) \leq \text{Sym}(G)$ (see also, [2, Theorem 7.2]). Then one can see that $\text{Cla}(G)$ forms a relatively prime equitable partition for \mathcal{X} in the sense of [10]. By Theorem 3.1 of that paper, any primitive fusion of the scheme \mathcal{X} must have rank 2. So, using the correspondence between the Cayley schemes and S-rings over G , one can show that G is a generalized B-group.

Let $G = G_1 \times G_2$ where G_1 and G_2 are groups of the same order $n > 1$. Then G is not a generalized B-group. Indeed, set $X_0 = \{(e_1, e_2)\}$ where e_i is the identity of G_i , and

$$X_1 = e_1 \times (G_2)^\# \cup (G_1)^\# \times e_2.$$

Denote by \mathcal{A} the span of the set $\{X_i : i = 0, 1, 2\}$ where X_2 is the complement to $X_0 \cup X_1$ in G . Then \mathcal{A} is, obviously, a central S-ring of rank 3 over G . Since it is also primitive, we are done.

Acknowledgment.

The paper was started during the visit of the third author to the Central China Normal University, Wuhan, China. He would like to thank the faculty members of the School of Mathematics and Statistics for their hospitality.

REFERENCES

- [1] P. P. Alejandro, R. A. Bailey, P. J. Cameron, *Association schemes and permutation groups*, Discrete Mathematics, **266** (2003), 47–67.
- [2] E. Bannai, T. Ito, *Algebraic combinatorics I: association schemes*, Benjamin-Cummings, Menlo Park, 1984.
- [3] A. R. Camina, *Some conditions which almost characterize Frobenius groups*, Israel Journal of Mathematics 31 (1978), 153–160.
- [4] S. Dolfi, A. Moretó, G. Navarro, *The groups with exactly one class of size a multiple of p*, J. Group Theory, 12(2009), 219–234.
- [5] S. Evdokimov, I. Ponomarenko, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, St. Petersburg Math. J., **14** (2003), no. 2, 189–221.
- [6] S. Evdokimov, I. Ponomarenko, *A new look at the Burnside-Schur theorem*, Bull. London Math Soc. 37(2005), 535–546.
- [7] W. Feit, G. M. Seitz, *On finite rational groups and related topics*, Illinois J. Math., **33** (1988), 103–131.
- [8] T. Feng, *Non-abelian skew Hadamard difference sets fixed by a prescribed automorphism*, J. Comb. Theory, **A118** (2011), No. 1, 27–36.
- [9] A. O. F. Hendrickson, *Supercharacter theories and Schur rings*, <http://arxiv.org/abs/1006.1363v1>, 2010, 1–17.
- [10] M. Hirasaka, H. Kang, K. Kim, *Characterization of association schemes by equitable partitions*, European J. Combin. 27 (2006), 139–152.
- [11] B. Huppert, *Character Theory of Finite Groups*, de Gruyter, 1998.
- [12] M. Muzychuk, I. Ponomarenko, *Schur rings*, European J. Combin., **30** (2009), 1526–1539.
- [13] I. Schur, *Zur Theorie der einfach transitiven Permutationgruppen*, S.-B. Preus Akad. Wiss. Phys.-Math. Kl. (1933) 598–623.
- [14] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.
- [15] H. Wielandt, *Permutation representations*, Ill. J. Math., **13** (1969), 91–94.

SCHOOL OF MATHEMATICS AND STATISTICS, CENTRAL CHINA NORMAL UNIVERSITY, WUHAN, CHINA

E-mail address: chengang19762002@aliyun.com

NETANYA ACADEMIC COLLEGE, NETANYA, ISRAEL

E-mail address: muzy@netanya.ac.il

STEKLOV INSTITUTE OF MATHEMATICS AT ST. PETERSBURG, RUSSIA

E-mail address: inp@pdmi.ras.ru